ASA/PIX 8.x. Пример конфигурации, разрешающей/блокирующей FTP-сайты при использовании регулярных выражений с MPF

Содержание

Введение

В настоящем документе описывается, как настроить защитные устройства Cisco Security Appliances ASA/PIX 8.x, которые используют регулярные выражения с системой модульных политик Modular Policy Framework (MPF) для того, чтобы блокировать/разрешать определенные FTP-сайты по имени сервера.

Предварительные условия

Требования

В данном документе предполагается, что устройство безопасности Cisco корректно настроено и работает нормально.

Используемые компоненты

Сведения, содержащиеся в этом документе, касаются следующих версий программного обеспечения и оборудования.

Устройство адаптивной защиты Cisco серии 5500 (ASA), на котором установлена версия ПО 8.0(x) или более поздняя

Cisco Adaptive Security Device Manager (ASDM) версии 6.x для ASA 8.x

Сведения для данного документа были получены на тестовом оборудовании в специально созданных лабораторных условиях. При написании данного документа использовались только устройства с "пустой" (стандартной) конфигурацией. При работе с реально функционирующей сетью необходимо полностью осознавать возможные результаты использования всех команд.

Условные обозначения

Более подробную информацию о применяемых в документе обозначениях см. в статье Cisco Technical Tips Conventions (Условные обозначения, используемые в технической документации Cisco).

Общие сведения

Обзор модульной системы политик

Модульная система политик (MPF) обеспечивает гибкий способ настройки параметров устройств безопасности. Например, MPF можно использовать для создания конфигурации с таймаутом, которая является специфичной для определенного TCP-приложения, в отличие от конфигураций, применимых ко всем TCP-приложениям.

MPF поддерживает функции, перечисленные ниже.

- Нормализация TCP, ограничение числа и продолжительности TCP- и UDP-соединений, а также рандомизация порядкового номера TCP
- CSC
- Контроль трафика на прикладном уровне
- IPS
- Входной контроль QoS
- Выходной контроль QoS
- Очередь с приоритетом QoS

Настройка MPF включает следующие 4 задачи.

- Определение трафика уровней 3 и 4, для которого требуется применить действия. Для получения подробной информации см. документ Определение трафика с использованием карты класса уровней 3/4.
- (Только для контроля трафика на прикладном уровне.) Указание специальных действий для контроля трафика на прикладном уровне. Для получения подробной

информации см. документ Задание специальных действий для контроля трафика на прикладном уровне.

Применение действий для трафика уровней 3 и 4. Для получения подробной информации см. документ Определение действий с использованием карты политик уровней 3/4.

Активация действий на интерфейсе. Для получения подробной информации см. документ Применение политики уровня 3/4 к интерфейсу с использованием служебной политики.

Регулярные выражения

Регулярное выражение либо точно соответствует текстовой строке, либо допускает использование метасимволов, позволяя совмещать различные варианты текстовой строки. Регулярные выражения можно использовать для совмещения контента определенного трафика приложений. Например, можно совместить строку URL внутри пакета HTTP.

Примечание. Чтобы исключить все специальные символы в командной строке, такие как вопросительные знаки (?) или табуляторы, используйте сочетание клавиш **Ctrl+V**. Например, используйте комбинацию **d[Ctrl+V]g**, чтобы ввести в конфигурацию **d?g**.

Для создания регулярных выражений используйте команду **regex**. Кроме того, команда **regex** может использоваться для реализации различных функций, требующих сравнения текста. Например, можно задать специальные действия для контроля приложения с использованием MPF и карты политик анализа. Для получения подробной информации см. команду **policy-map type inspect**.

На карте политик анализа можно задать трафик, используемый при создании карты классов анализа, которая содержит одну или несколько команд **match**. Можно также использовать команды **match** непосредственно в карте политик анализа. Некоторые команды **match** позволяют идентифицировать текст в пакете, используя регулярное выражение. Например, можно совместить строки URL внутри пакетов HTTP. Можно группировать регулярные выражения в соответствующую карту класса. Для получения подробной информации см. команду **class-map type regex**.

Следующая таблица содержит список метасимволов, имеющих специальное значение.

Символ	Описание	Примечания
.	Точка	Соответствует любому одиночному символу. Например, выражению **d.g** соответствуют слова dog, dag, dtg, а также любое слово, содержащее эти символы, например, «doggonnit».
(exp)	Вложенное выражение	Вложенное выражение отделяет символы от окружающего текста, позволяя использовать внутри скобок другие метасимволы. Например, выражению **d(o|a)g**

		соответствуют слова dog и dag, в то время как выражению **do|ag** соответствуют do и ag. Вложенные выражения могут также использоваться с кванторами повторения для указания числа повторяющихся знаков. Например, выражению **ab(xy){3}z** удовлетворяет последовательность abxyxyxyz.
|	Дизъюнкция (логическое сложение)	Соответствует любому из разделенных им выражений. Например, выражению **dog|cat** удовлетворяет как слово dog, так и слово cat.
?	Вопросительный знак	Квантор, указывающий, что предшествующее ему выражение может встречаться 0 или 1 раз. Например, выражению **lo?se** соответствуют строки «lse» и «lose». **Примечание.** Чтобы набрать вопросительный знак, перед ним необходимо нажать **Ctrl+V** в противном случае будет вызвана функция справки.
*	Звездочка	Квантор, указывающий, что предшествующее ему выражение может встречаться 0, 1 или произвольное число раз. Например, выражению **lo*se** соответствуют строки lse, lose, loose и т. д.
{x}	Квантор повторения	Повторяет символы ровно x раз. Например, выражению **ab(xy){3}z** удовлетворяет последовательность abxyxyxyz.
{x,}	Квантор минимального повторения	Повторяет символы не менее x раз. Например, выражению **ab(xy){2,}z** удовлетворяют последовательности «abxyxyz», «abxyxyxyz» и т. д.
[abc]	Класс символа	Соответствует любому символу в квадратных скобках. Например, выражению **[abc]** удовлетворяют символы a, b и c.
[^abc]	Отрицание класса символа	Соответствует одному символу, не содержащемуся в квадратных скобках. Например, выражению **[^abc]** удовлетворяет любой из знаков, кроме a, b и c. **[^A-Z]**

		соответствует любому одиночному знаку, который не является латинской буквой в верхнем регистре.
[a-c]	Класс диапазона символов	Соответствует любому символу в определенном диапазоне. **[a-z]** соответствует любой букве в нижнем регистре. Символы и диапазоны можно сочетать: **[abcq-z]** соответствует знакам a, b, c, q, r, s, t, u, v, w, x, y, z, как и выражение **[a-cq-z]**. Внутри квадратных скобок знак тире (-) воспринимается как таковой только в том случае, если он стоит первым или последним: **[abc-]** или **[-abc]**.
""	Кавычки	Позволяют указать пробелы в начале или конце строк. Например, выражение **" test"** обрабатывается с учетом стоящего в начале пробела.
^	Вставка	Указывает, что выражение должно начинаться с начала строки.
\	Подтверждение символа	В сочетании с метасимволом указывает, что последний должен восприниматься как обычный символ. Например, выражению **\[** соответствует открывающая квадратная скобка.
char	Символ	Если знак не является метасимволом, он воспринимается как обычный символ.
\r	Возврат каретки	Соответствует символу возврата каретки: 0x0d.
\n	Перевод строки	Соответствует символу перевода строки: 0x0a.
\t	Табулятор	Соответствует табулятору: 0x09.
\f	Новая страница	Соответствует символу новой страницы: 0x0c.
\xNN	Шестнадцатеричная нумерация	Соответствует символу ASCII с указанным кодом в шестнадцатеричном виде (код должен содержать строго две цифры).
\NNN	Восьмеричная нумерация	Соответствует символу ASCII с указанным кодом в восьмеричном виде (код должен

		содержать строго три цифры). Например, код 040 соответствует пробелу.

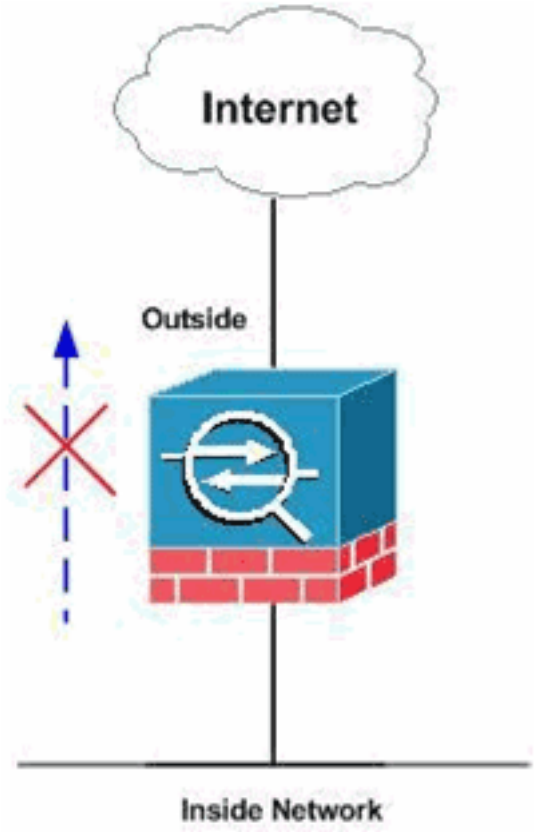
Конфигурация

В этом разделе приводятся сведения о настройке функций, описанных в данном документе.

Примечание. Для поиска дополнительной информации о командах, приведенных в данном документе, используйте инструмент Command Lookup Tool (только для зарегистрированных пользователей).

Сетевой график

В этом документе используется следующая схема сети.



Примечание. Выбранные FTP-сайты разрешаются или блокируются с помощью регулярных выражений.

Конфигурации

В этом документе используются следующие конфигурации:

- Конфигурация ASA в интерфейсе командной строки
- Конфигурация ASA 8.x с ASDM 6.x

Конфигурация ASA в интерфейсе командной строки

Конфигурация ASA в интерфейсе командной строки

```
ciscoasa#show run
: Saved
:
ASA Version 8.0(4)
!
hostname ciscoasa
domain-name cisco.com
enable password 8Ry2YjIyt7RRXU24 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
names
!
interface GigabitEthernet0/0
 nameif outside
 security-level 0
 ip address 10.66.79.86 255.255.255.224
!
interface GigabitEthernet0/1
 nameif inside
 security-level 100
 ip address 10.238.26.129 255.255.255.248
!
interface Management0/0
 shutdown
 no nameif
 no security-level
 no ip address
!
!---    (regex),   FTP,   !--- .  .   ,   ,   !---  220,
 .     !--- URL,   . , !---  FTP: 220
g1u0103c.austin.hp.com


regex FTP_SITE1 "([0-9A-Za-z])*[Hh][Pp]\.[Cc][Oo][Mm]"
regex FTP_SITE2 "([0-9A-Za-z])* CISCO SYSTEMS ([0-9A-Za-
z])*"

!---  .         !---   220 ( , ,    FTP !---   ,   ,  !-
--    ).


boot system disk0:/asa804-k8.bin
ftp mode passive
pager lines 24
logging enable
logging timestamp
logging buffered debugging
mtu outside 1500
mtu inside 1500
no failover
icmp unreachable rate-limit 1 burst-size 1
asdm image disk0:/asdm-61557.bin
no asdm history enable
arp timeout 14400

global (outside) 1 interface
nat (inside) 1 0.0.0.0 0.0.0.0
route outside 0.0.0.0 0.0.0.0 10.66.79.65 1

timeout xlate 3:00:00
```

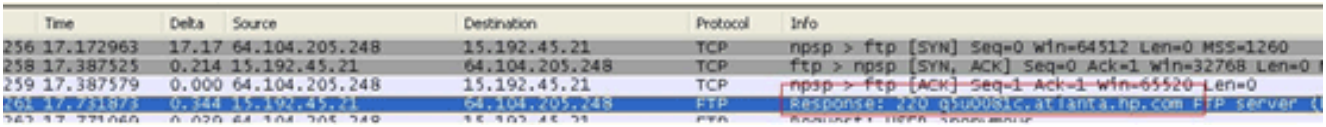
```
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00
icmp 0:00:02
timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp
0:05:00 mgcp-pat 0:05:00
timeout sip 0:30:00 sip_media 0:02:00 sip-invite 0:03:00
sip-disconnect 0:02:00
timeout sip-provisional-media 0:02:00 uauth 0:05:00
absolute
dynamic-access-policy-record DfltAccessPolicy

http server enable
http 0.0.0.0 0.0.0.0 inside
http 0.0.0.0 0.0.0.0 outside
no snmp-server location
no snmp-server contact
snmp-server enable traps snmp authentication linkup
linkdown coldstart

telnet timeout 5
ssh scopy enable
ssh timeout 5
console timeout 0
management-access inside
threat-detection basic-threat
threat-detection statistics access-list
no threat-detection statistics tcp-intercept


class-map type regex match-any FTP_SITES
 match regex FTP_SITE1
 match regex FTP_SITE2

!  ,      !  FTP,        (regex). class-map type inspect
ftp match-all FTP_class_map
 match not server regex class FTP_SITES

!     FTP      !---  ,  ,  FTP  . .  ,    !---   ,
regex, !---     match not.    !---   FTP,   match    not
.


class-map inspection_default
 match default-inspection-traffic

policy-map type inspect dns preset_dns_map
 parameters
  message-length maximum 512

policy-map type inspect ftp FTP_INSPECT_POLICY
 parameters
 class FTP_class_map
  reset log

!  ,    ,   !--- ,   . policy-map global_policy class
inspection_default inspect dns preset_dns_map inspect
h323 h225 inspect h323 ras inspect netbios inspect rsh
inspect rtsp inspect skinny inspect esmtp inspect sqlnet
inspect sunrpc inspect tftp inspect sip inspect xdmcp
inspect icmp inspect ftp strict FTP_INSPECT_POLICY

!---  FTP    , !---     . service-policy global_policy
global prompt hostname context
Cryptochecksum:40cefb1189e8c9492ed7129c7577c477 : end
```

Конфигурация ASA 8.x с ASDM 6.x

Выполните следующие шаги, чтобы задать регулярные выражения и применить их к MPFдля блокирования определенных FTP-сайтов.

Определение имени сервера FTP.

Система проверки FTP может использовать различные критерии, такие как команда, имя файла, тип файла, сервер и имя пользователя. В данной процедуре в качестве критерия используется сервер. Система проверки FTP использует ответ 220, отправляемый FTP-сайтом, в качестве значения сервера. Это значение может отличаться от имени домена, используемого сайтом. В этом примере используется Wireshark для захвата пакетов FTP проверяемого сайта, чтобы получить значение ответа 220 на регулярное выражение, использованное в шаге 2.

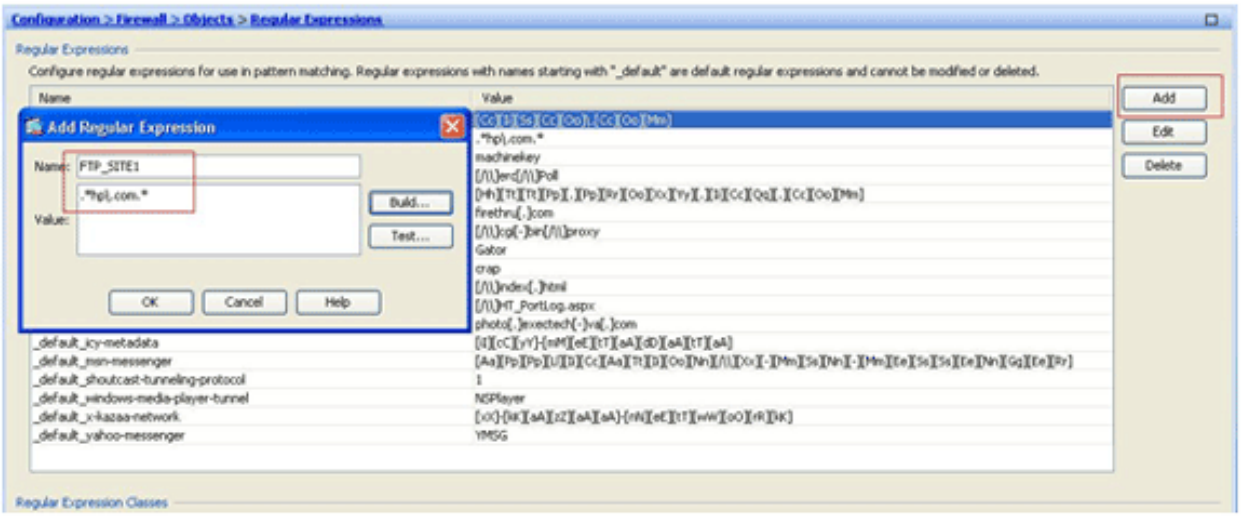


Основываясь на получении ответа 220, значение для ftp://hp.com будет (например) *q5u0081c.atlanta.hp.com*.

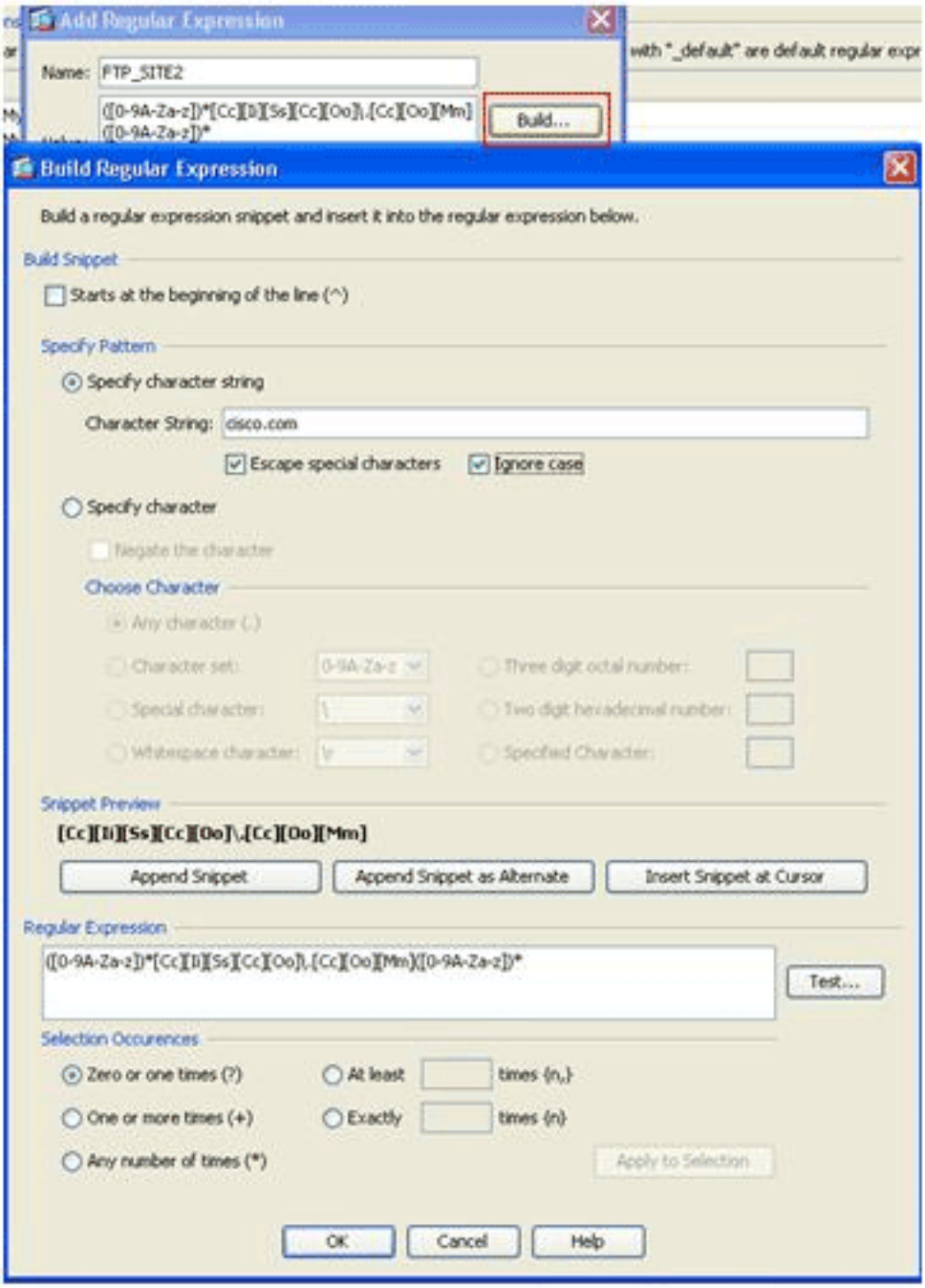
Создание регулярных выражений.

Выберите **Configuration > Firewall > Objects > Regular Expressions** (Конфигурация > Межсетевой экран > Объекты > Регулярные выражения) и нажмите **Add** (Добавить) на вкладке Regular Expression, чтобы создать регулярное выражение, как описано в данной процедуре.

Создайте регулярное выражение *FTP_SITE1*, чтобы сравнить ответ 220 (наблюдаемый при захвате пакетов в Wireshark или в другом используемом инструменте), полученный с FTP-сайта (например, ".* hp\.com.*") и нажмите **OK**.



Примечание. Можно нажать **Build** (Создать), чтобы получить справку о том, как создавать более сложные регулярные выражения.

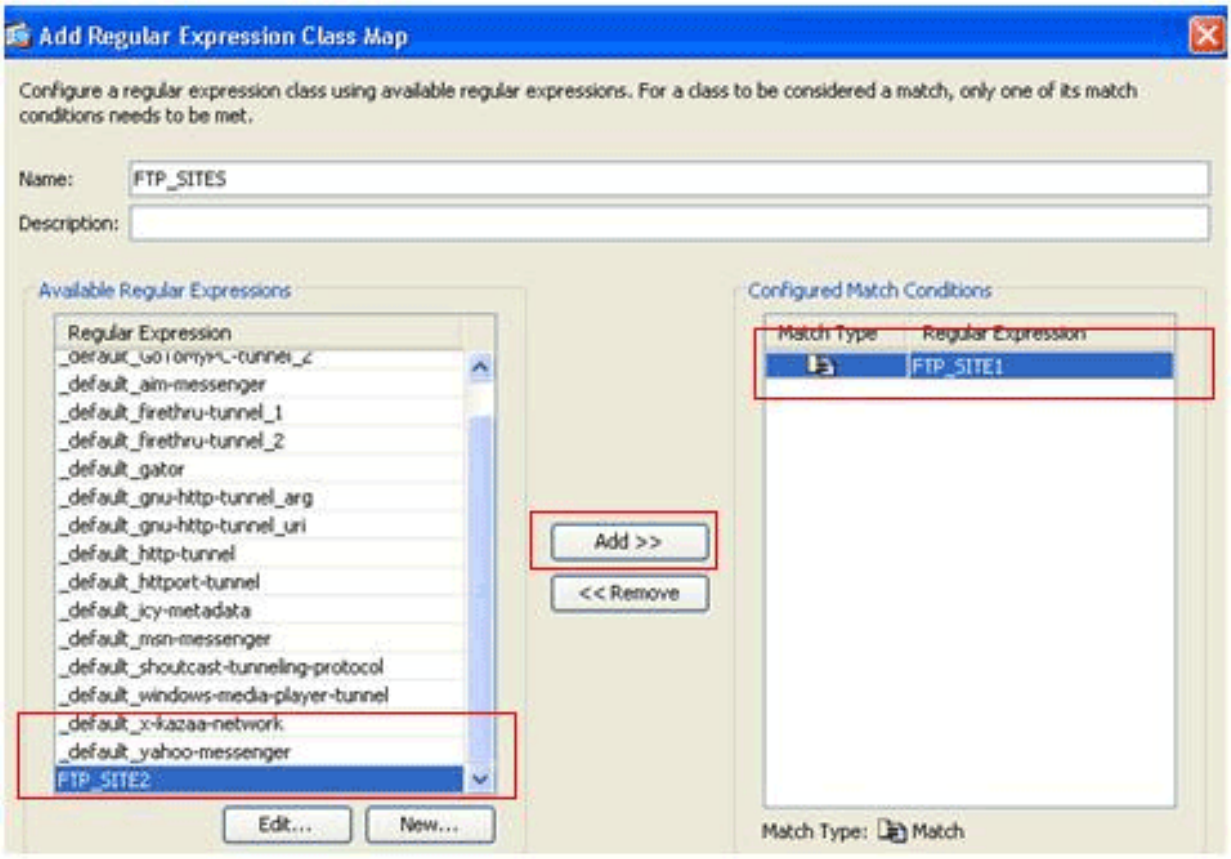


После создания регулярного выражения нажмите **Apply** (Применить).

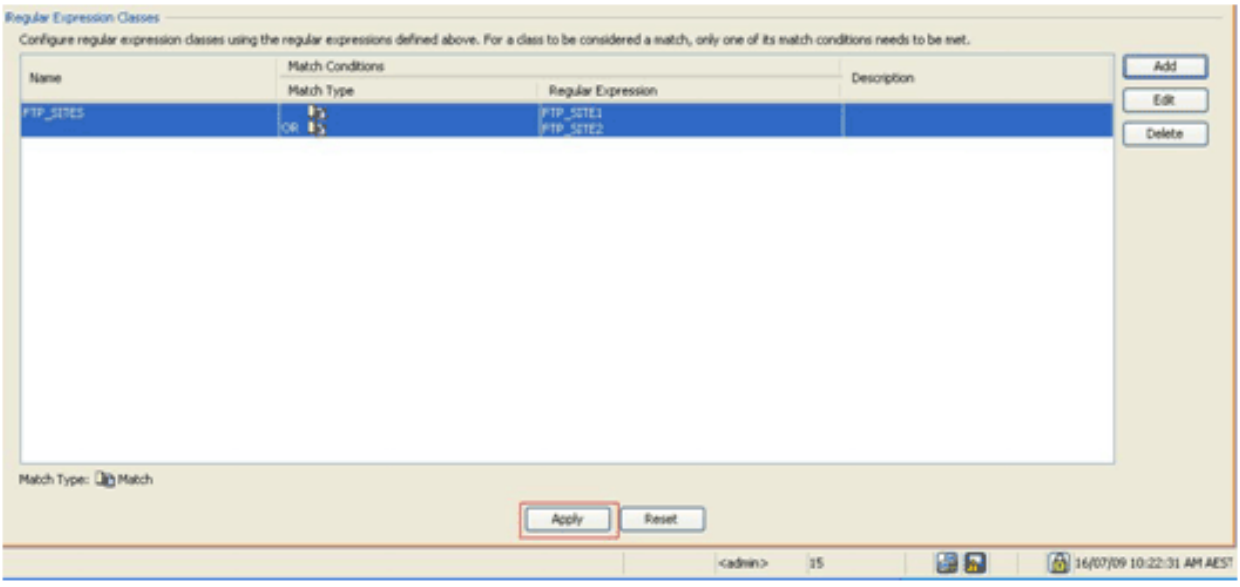
Создание классов регулярных выражений.

Выберите **Configuration > Firewall > Objects > Regular Expressions** и нажмите **Add** в разделе Regular Expression Classes, чтобы создать класс регулярных выражений, как описано в данной процедуре.

Создайте класс регулярных выражений *FTP_SITES*, чтобы он соответствовал обоим выражениям *FTP_SITE1* и *FTP_SITE2* и нажмите **OK**.



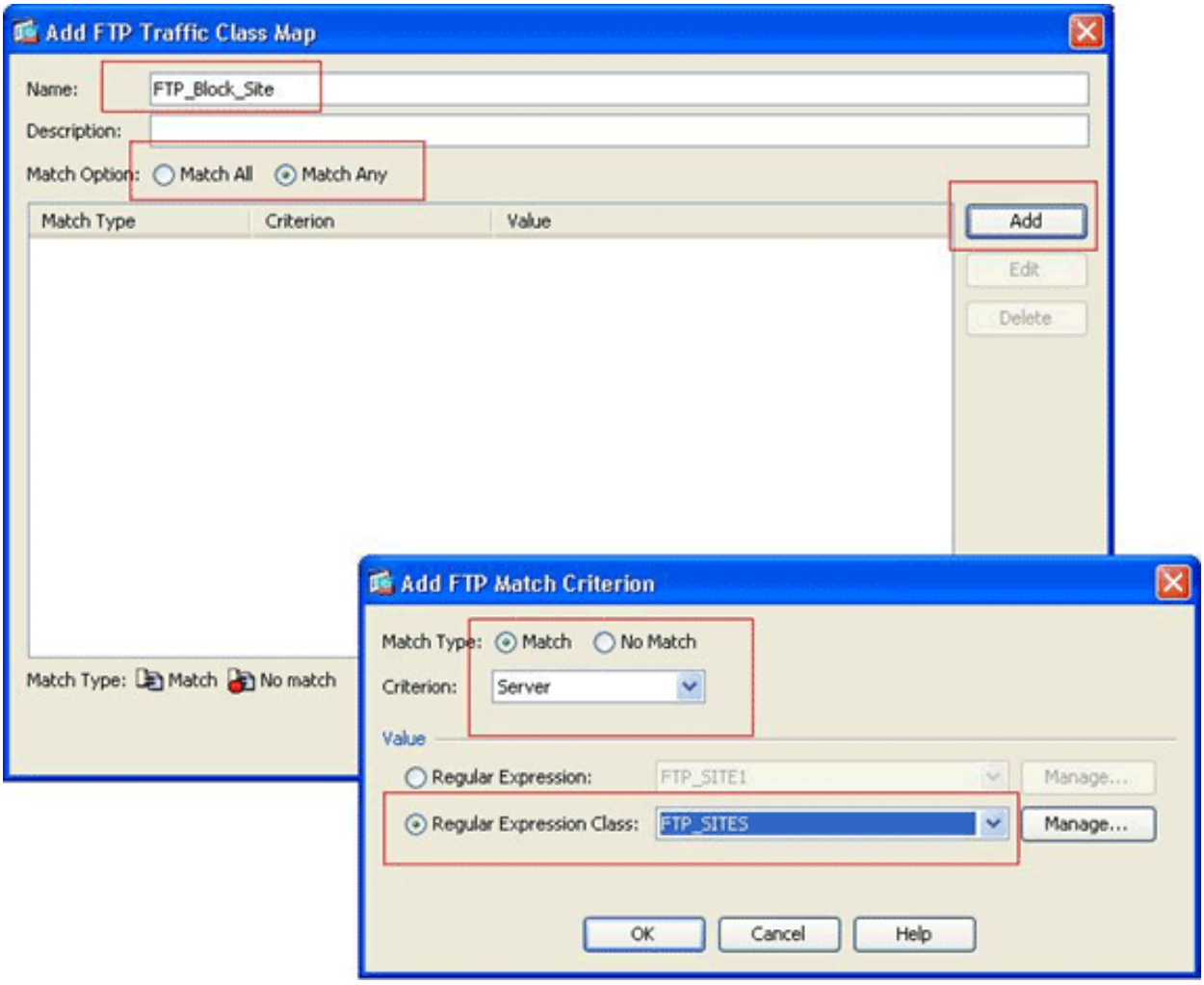
После создания карты класса нажмите **Apply**.



Проверка указанного трафика с помощью карт класса.

Выберите **Configuration > Firewall > Objects > Class Maps > FTP > Add**, нажмите правую кнопку мыши и выберите **Add**, чтобы создать карту класса для проверки трафика FTP, идентифицированного различными регулярными выражениями, как описано в данной процедуре.

Создайте карту класса *FTP_Block_Site*, чтобы он соответствовал ответу 220 FTP с созданными регулярными выражениями.



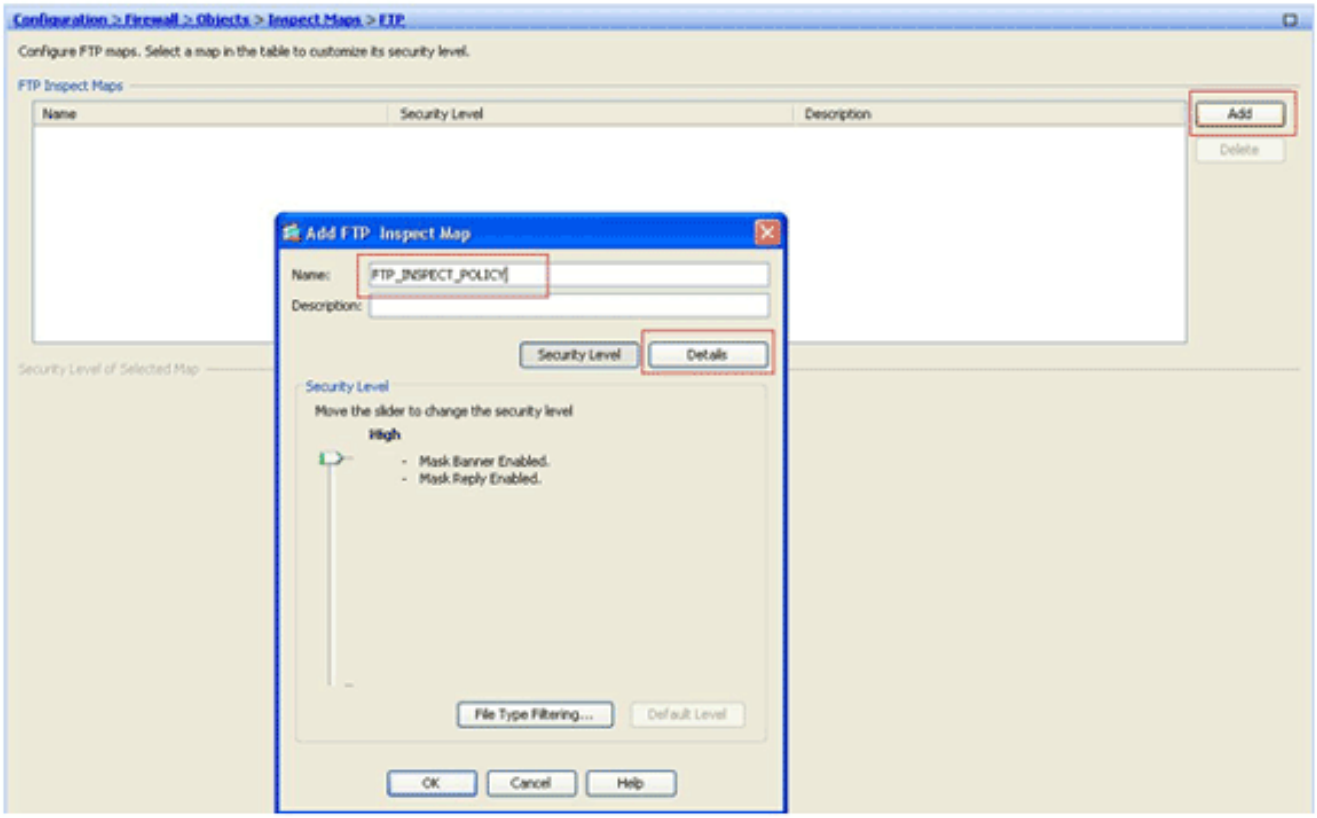
Если требуется исключить сайты, заданные в регулярном выражении, нажмите кнопку **No Match** (Отсутствие соответствия).

В разделе Value (Значение) выберите либо регулярное выражение, либо класс регулярных выражений. Для данной процедуры выберите ранее созданный класс.

Нажмите кнопку **Apply**.

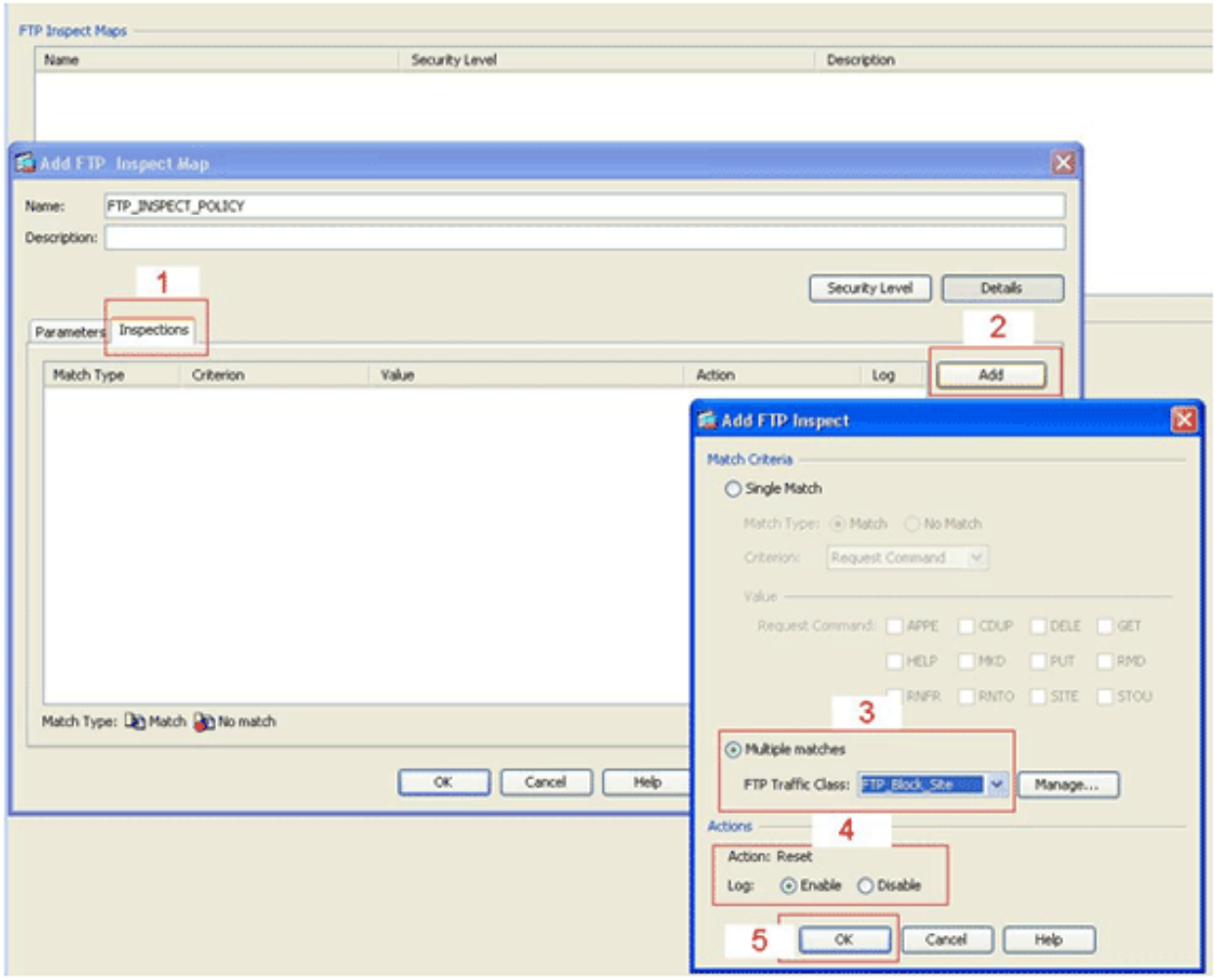
Задание действий для проверяемого трафика в политике анализа.

Выберите **Configuration > Firewall > Objects > Inspect Maps > FTP> Add**, чтобы создать политику анализа и задать необходимое действие для проверяемого трафика.



Введите имя и описание политики анализа. (Например, *FTP_INSPECT_POLICY*.)

Нажмите кнопку **Details** (Сведения).



Перейдите на вкладку **Inspections** (Проверки). (1)

Нажмите кнопку **Add** (Добавить). (2)

Нажмите кнопку **Multiple matches** (Множественные совпадения) и выберите класс трафика в раскрывающемся списке. (3)

Выберите необходимое действие переустановки для разрешения или блокировки. В этом примере разрешается FTP-подключение с переустановкой для всех FTP-сайтов, *не соответствующих* заданным сайтам. (4)

Нажмите **OK**, затем снова **OK** и **Apply**. (5)

Добавление политики проверки FTP к списку глобальной проверки.

Выберите **Configuration > Firewall > Service Policy Rules**.

Справа выберите политику **inspection_default** и нажмите **Edit** (Правка).

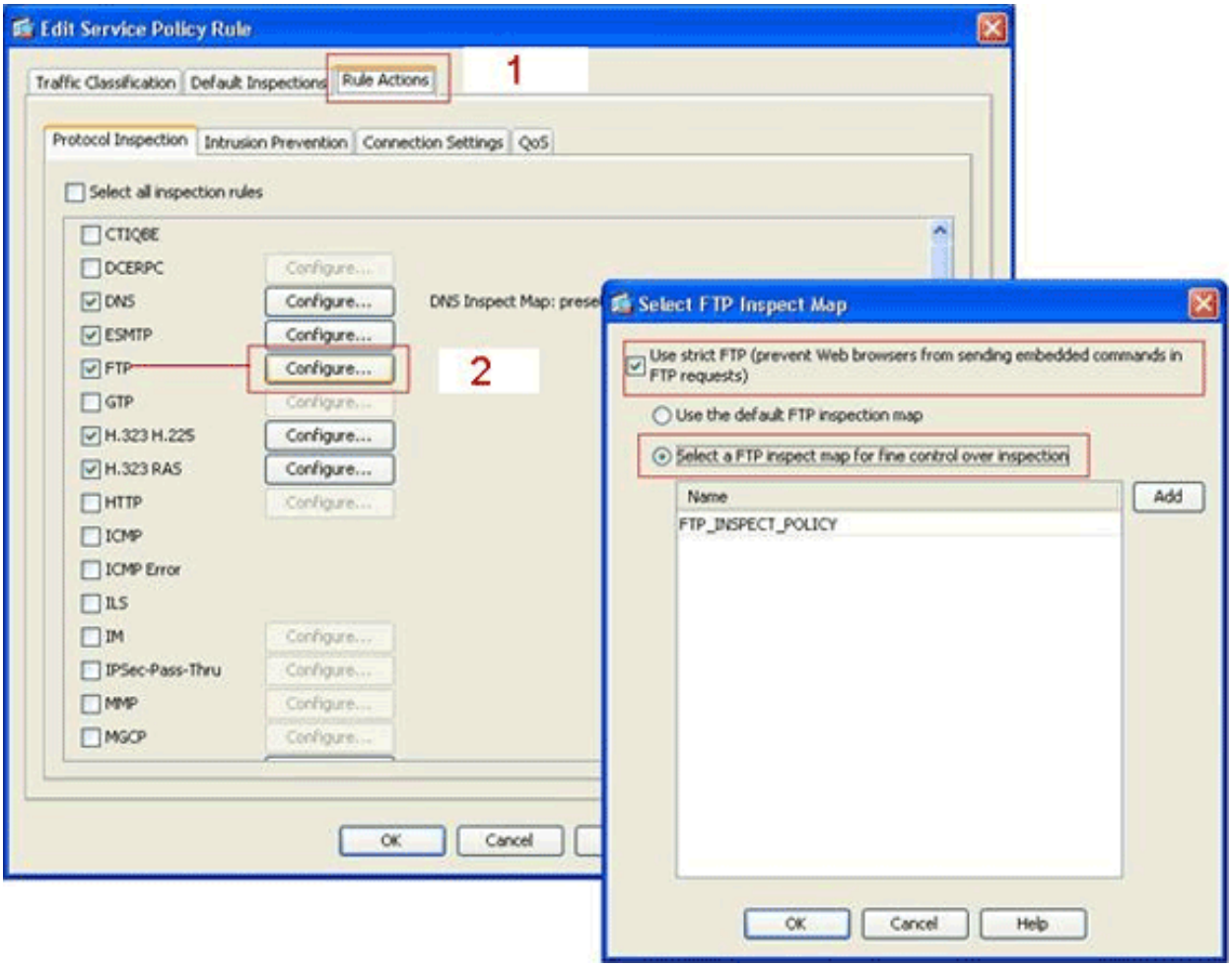
На вкладке Rule Actions (Действия правила) (1) нажмите для FTP кнопку **Configure**

(Настроить). (2)

В диалоговом окне Select FTP Inspect Map (Выбор карты проверки FTP) установите флажок **Use strict FTP** (Использовать точный FTP), затем нажмите кнопку **FTP inspect map for fine control over inspection** (Карта проверки FTP для точного контроля после проверки).

Новая политика проверки FTP, *FTP_INSPECT_POLICY*, должна отображаться в списке.

Нажмите **OK**, затем снова **OK** и **Apply**.



Проверка

Используйте этот раздел для того, чтобы подтвердить, что ваша конфигурация работает правильно.

Средство Output Interpreter Tool (OIT) (только для зарегистрированных клиентов) поддерживает определенные команды **show**. Используйте средство OIT для анализа выходных данных команд **show**.

show running-config regex — данная команда показывает созданные конфигурации регулярных выражений.

```
ciscoasa#show running-configregex
regex FTP_SITE1 "[Cc][Ii][Ss][Cc][Oo]\.[Cc][Oo][Mm]"
regex FTP_SITE2 ".*hp\.com.*"
```

show running-config class?map — данная команда показывает созданные конфигурации карт классов.

```
ciscoasa#show running-config class-map
class-map type regex match-any FTP_SITES
 match regex FTP_SITE1
 match regex FTP_SITE2
class-map type inspect ftp match-all FTP_Block_Site
 match not server regex class FTP_SITES
class-map inspection_default
 match default-inspection-traffic
!
```

show running-config policy-map type inspect http — данная команда показывает созданные конфигурации карт политик для проверки трафика HTTP.

```
ciscoasa#show running-config policy-map type inspect ftp
!
policy-map type inspect ftp FTP_INSPECT_POLICY
 parameters
  mask-banner
  mask-syst-reply
 class FTP_Block_Site
  reset log
 !
```

Show running-config policy-map — данная команда показывает все конфигурации карт политик, а также конфигурации карт политик по умолчанию.

```
ciscoasa#show running-config policy-map
!
policy-map type inspect dns preset_dns_map
 parameters
  message-length maximum 512
policy-map type inspect ftp FTP_INSPECT_POLICY
 parameters
  mask-banner
  mask-syst-reply
 class FTP_Block_Site
  reset log
policy-map global_policy
 class inspection_default
  inspect dns preset_dns_map
  inspect h323 h225
  inspect h323 ras
  inspect netbios
```

```
  inspect rsh
  inspect rtsp
  inspect skinny
  inspect esmtp
  inspect sqlnet
  inspect sunrpc
  inspect tftp
  inspect sip
  inspect xdmcp
  inspect ftp strict FTP_INSPECT_POLICY
!
```

show running-config service-policy — данная команда показывает все выполняемые в настоящее время конфигурации политик служб.

```
ciscoasa#show running-config service-policy
service-policy global_policy global
```

Поиск и устранение неполадок

В этом разделе описывается процесс устранения неполадок конфигурации.

Чтобы проверить корректность выполнения проверки трафика системой и точность разрешения и блокировки, можно использовать команду **show service-policy**.

```
ciscoasa#show service-policy

Global policy:
  Service-policy: global_policy
    Class-map: inspection_default
      Inspect: dns preset_dns_map, packet 0, drop 0, reset-drop 0
      Inspect: h323 h225 _default_h323_map, packet 0, drop 0, reset-drop 0
      Inspect: h323 ras _default_h323_map, packet 0, drop 0, reset-drop 0
      Inspect: netbios, packet 0, drop 0, reset-drop 0
      Inspect: rsh, packet 0, drop 0, reset-drop 0
      Inspect: rtsp, packet 0, drop 0, reset-drop 0
      Inspect: skinny , packet 0, drop 0, reset-drop 0
      Inspect: esmtp _default_esmtp_map, packet 0, drop 0, reset-drop 0
      Inspect: sqlnet, packet 0, drop 0, reset-drop 0
      Inspect: sunrpc, packet 0, drop 0, reset-drop 0
      Inspect: tftp, packet 0, drop 0, reset-drop 0
      Inspect: sip , packet 0, drop 0, reset-drop 0
      Inspect: xdmcp, packet 0, drop 0, reset-drop 0
      Inspect: ftp strict FTP_INSPECT_POLICY, packet 40, drop 0, reset-drop 2
```